DOCUMENT RESUME

ED 290 428 IR 012 976

AUTHOR Clark, Orvin R.
TITLE Computer Disaster Recovery Planning.
PUB DATE 22 Oct 86
NOTE 23p.; Paper presented at the Annual International Meeting of the American Society of Business Officers (San Francisco, CA, October 22, 1986).
PUB TYPE Guides - Non-Classroom Use (055) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS Computers; *Computer Software; *Data Processing; Educational Administration; Educational Planning; *Emergency Programs; Guidelines; Insurance
IDENTIFIERS *Disaster Planning; Environmental Control; *Power Failures

ABSTRACT

Arguing that complete, reliable, up-to-date system documentation is critical for every data processing environment, this paper on computer disaster recovery planning begins by discussing the importance of such documentation both for recovering from a systems crash, and for system maintenance and enhancement. The various components of system documentation are then explained, followed by descriptions of the three stages of creation of complete system documentation: (1) design and development documentation; (2) backup documentation; and (3) documentation reports. Environmental controls, a second major aspect of disaster recovery planning, are then discussed, with emphasis on problems with the electrical power supply such as "blinks," "brownouts," and "blackouts." Ways to ensure an uninterruptable power supply, voltage tolerance of the computer's chart, and sources of assistance are also considered. A discussion of safeguards that can be used to protect the data processing system, including various kinds of insurance, concludes the paper. (RP)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☒ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

ED290428

COMPUTER DISASTER RECOVERY PLANNING

ORVIN R. CLARK, RSBA

ASSISTANT SUPERINTENDENT - BUSINESS

COMMUNITY UNIT SCHOOL DISTRICT 220

BARRINGTON, ILLINOIS

PRESENTED AT THE

ASBO INTERNATIONAL ANNUAL MEETING

SAN FRANCISCO, CALIFORNIA

OCTOBER 22, 1986

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Orvin R. Clark

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

BEST COPY AVAILABLE

IR012976

DEFINITIONS:

DISASTER

(1) a sudden or grievous misfortune

(2) an unforeseen mischance

(3) utter defeat

(4) catastrophic event

(5) computer secretary resigns

RECOVERY

(1) Regain

(2) Reclaim

(3) Restore

(4) Collect Insurance

(5) After a "crash"

PLANNING

(1) implies mental formulation

(2) provides graphic representation

(3) emphasizes scope and vision

(4) establishes order and harmony

(5) Business Manager saves job w/DRP

NOTE: Read all number 5's continuously as in a sentence!

2.

TITLE **COMPUTER DISASTER RECOVERY PLANNING**

SUBTITLE PREPARING FOR DISASTER

POINT Just in case you need it --- Your job, that is!

COUNTER POINT: **MURPHY'S LAW** - IF IT IS POSSIBLE FOR SOMETHING TO GO WRONG -- IT WILL AT THE MOST INCONVENIENT TIME

SCENARIO "The system has never failed"
I'm sure your School Board and Superintendent will understand when you explain that you didn't have

time to develop a DRP, now that the system has crashed and payday is today, but payroll should be ready for distribution in five days.

PROBLEM IDENTIFICATION Need a computer Disaster Recovery Plan

PROBLEM SOLUTION A manager's viewpoint on Computer DRP

INTRO " What You Don't Have Will Hurt You"

DR PLAN OUTLINE

3.

1. SYSTEM DOCUMENTATION

A. WHAT IS IT?

1. Program (application) purpose description
2. File layouts
3. Flowcharts
4. Program Processing Description
5. Procedure, object code and source program listings
6. Test Results
7. Program and File cross reference listings
8. User manual
9. Control manual
10. Backup tape or diskettes

B. DESIGN & DEVELOPMENT DOCUMENTATION

1. Program/function Description
2. Flowcharts
3. Source Code listing

C. BACKUP DOCUMENTATION

1. Copy of:
    a. data file
    b. library
    c. program
    d. procedure
2. Frequency (daily/weekly)
3. Off-site storage (rotation)
4. Reciprocal Agreement
5. Specimens - FP-B SD

4.

D. DOCUMENTATION REPORTS

1. Program Source Listing

2. Other Reports

a. Glossary

b. Cross Reference

c. Printer spacing charts

d. menu

e. procedure listing

3. Software Documentors

a. Automatically produces reports

b. Available software houses

2. ENVIRONMENTAL CONTROLS

A. AIR CONDITIONING (most common)

B. POWER PROTECTION ("quality of power supply")

1. Power Problems

A. Identify type

1. "Blink" - heavy loading line switch (1/2 second)

2. "Brownouts" - imposed voltage reductions

3. "Blackouts" - unscheduled voltage outage

B. UPS - Uninterruptable Power Supply

1. Battery Backup System - standby (Lag)

2. Battery Backup System - On line (Expensive)

5.

2. Voltage tolerances of Computer's chart (U.S. DOC.) Identified:

A. Typical Computer requirements

B. Typical Utility Power

C. Possible Power Received

D. Possible Results of Power Problem

In comparison to:

A. Steady State Voltage

B. Transient Voltage

C. Voltage Continuity

D. Frequency

C. Assistance

1. Computer Manufacturer

2. Computer Power Conditioning and backup equipment vendor

3. U.S. Dept. of Commerce

3. **SAFEGUARDS**

A. OCCURRENCES (main vs. micro)

1. Computer Center Claims (Specific Risk Policies)

A. Water 35%

B. Vandalism & Malicious damage 20%

2. Micro computers (All risk Policies)

A. Theft 50%

B. Power surges 33%

B. INSURANCE (hardware and software)

1. Property
2. Business Interruption
3. Extra Expense
4. Computer Crime
5. Errors and Omissions
6. Fidelity

C. ALL OTHER ABOVE

D. PRUDENT MANAGER - Whatever the size or system in use as reliance on computers continue to grow, so does the need to protect computers (hardware and software).

4. SUMMARY

A. AFTER CRASH

B. FIND DRP

C. HAPPY ENDING

COMPUTER DISASTER RECOVERY PLANNING

INTRODUCTION

"What you don't have will hurt you."

Business Managers, DP Managers, Programmers and Systems Operators know it, but almost no one does anything about it -- until it's too late.

Complete, reliable, up-to-date system documentation is critical for every data processing environment.

Systems crash - that's a fact of data processing life. At any moment, programs of data can be accidentally altered or destroyed without warning. Power failure, fire, flood, vandalism, operator error, operator ignorance, sabotage, burst pipes, hardware failure, conversion problems, programming errors and other assorted acts of God and man can damage the integrity of data before anybody knows what happened.

You need good system documentation for two reasons. First, and most important, is that you can recover from a system crash. Reliable documentation makes recovery an inconvenience rather than a catastrophe. Lost data is quickly replaced and down time is minimal. Lack of up-to-date, usable system documentation results in not only lost data and hours of extra work, but also lost tempers, confusion, and data processing chaos.

The second reason is so that you can maintain the system. Fortunately, program modifications are far more common than power failures and floods. Good documentation allows another programmer to follow logic and flow of program in order to de-bug or enhance it.

All to often, system documentation is an afterthought and only an issue when another programmer tries to modify a program. There is so much pressure on data processing departments to get the job done and out the door that there is little time for documentation.

Usually, what documentation does exist is little more than a source code listing, a program diskette and a user's manual. That may be enough to install the system, but not enough for recovery from a system failure or for maintenance.

Programmers themselves contribute to the lack of good documentation. Programmers like to program, they don't to spend time writing documentation. Furthermore, some programmers certainly want to protect what they consider privileged information. They don't want to make enhancements or modifications easy for other programmers. It's built-in job security! (emphasis)

What is it.

System documentation means different things to different people. A DP Manager may think system documentation includes complete source listings. Programmers may think that comment lines in each programs

are enough. The system operator needs a collection of backup tapes and diskettes and technical support personnel want clear and concise user manuals.

System documentation is all of these things and more. The very essentials of adequate system documentation are:

1. Up-to-date source listing
2. File Layouts
3. Backup Tapes and diskettes

These make recovery from a crash and program modification enhancements possible, but far from painless. Complete system documentation includes the following 10 ingredients:

1. Program or application purpose general description: General description of the purpose of the program or application.
2. File Layouts: Layout specifications, data base details and other information necessary for execution of the program.
3. Flow Charts: Flow charts showing where each program fits into an application or system.
4. Program Processing Description: Detailed description of the processing that takes place within the program.
5. Procedure Code and Source Listings: Procedure, object code and source listings.
6. Test Results: Data used to test the program including test results.

7. Cross Reference Listings: Program and File Cross reference listing.
8. User Manual: User Manual that describes how data is entered, updated and manipulated within the system.
9. Control Manual: Control Manual that describes how the program or application is used within the system.
10. Backup: Backup tapes and diskettes (including off site storage)

The complete system documentation requires three stages of creation. Design and development, backup and reports.

DESIGN AND DEVELOPMENT DOCUMENTATION. Design and Development Documentation is the first step toward complete documentation. During system design, a general description of the program and its function is written, including a summary of the program's functions and features and the user's benefits that result from the program.

Once the overall plan of the program is developed, a flow chart is created that illustrates how the program works. Another flow chart shows how the program fits into the rest of the system. For example, an Accounts Payable application has a flow chart of its own, but it is also shown in its relationship to the general ledger, accounts payable, inventory and purchasing systems. The flow charts graphically present the program and how it works.

The most important part of system documentation in the design and development stage is writing comments into the source code while the

program is being written and is fresh in the mind of the programmer. Any comments in the program after it is written, always takes more time and increases the chance for error. Once the program is written there never seems to be adequate time to do the comments justice.

The source listing can be a gold mine of comments that describe each step of the processing or it can be a jigsaw puzzle that meanders through loops to arrive at a conclusion. Comments written into the source program are valuable sign posts that guide readers through each processing step. No two programmers solve a problem or write a program the same. Simple, clear comments in the program will help the programmer's logic and flow of processing.

BACKUP DOCUMENTATION: Backup documentation is a copy of a data file, procedure, program or library on a tape or diskette. The responsibility for backup documentation lies with both the system operator and user. As a matter of good processing procedure, the system operator should regularly copy files and libraries to a tape or diskette in case data or programs are accidentally altered or lost due to power loss, human error or some other event. The frequency of system backup is dictated by circumstances.

The end user should, however, be responsible for more frequent backups of specific applications and files. For example, it may be necessary to back up the general ledger transaction file twice a day to ensure the integrity of the data. It is unreasonable to ask a system operator to back up a specific file twice a day, every day. The end

user can easily and quickly back it up. Then if a file needs to be restored, the user knows the exact location and contents of the most recent data. When the file is stored, the amount of time lost is minimal.

Tapes and diskettes made as system backup documentation should be stored off site in a safe place. Many organizations store backup documentation in a safe deposit box or another organization's vault. Backup documentation that remains on site runs the risk of being lost in a fire or flood along with the system it is supposed to protect. The specimens of a backup procedure and off site storage rotation as well as a reciprocal agreement are part of the outline that is available after the presentation.

DOCUMENTATION REPORTS: After a program is written and tested, it's time to print out documentation reports. Documentation reports are listings that provide hard copies of procedures and programs and serve as file, program and procedure cross-references.

The basic documentation report is a source listing of the program. That, by itself, provides a means of recovery in case of a system crash and enables program modification by another programmer. Other documentation reports describe various parts of the system and their relationship with the whole. For example:

Field Name Glossary describes every field used by every file. Files are presented in alphabetical order with the file name, program name,

from/to positions and attributes.

Program by File Cross-reference: report lists the programs used by each file.

File by Program Cross-reference: reports lists of files used by each program.

Nested Procedure Analysis: lists each program called by a menu and shows the other lower level procedures it calls.

Program by Program Cross-reference: lists the procedures used by each program.

Printer Spacing Charts: provide a layout of each report format in the program.

Menu Cross-reference: shows the procedures called by each menu option.

Procedure Listing: is a hard copy of the procedures in the program.

This is only a sample of the types of reports that can be created for every program. Information provided by these reports makes systems easy for other programmers to learn and modify.

There is no need to write programs to create documentation. Software

is available from equipment manufacturers and software houses which automatically produce documentation reports for any library on disk.

Documentation requires a commitment for managers, designers, programmers and users to include documentation writing time and programming schedules. But it is the manager's responsibility for a system who must make sure that designers properly describe it, that programmers include meaningful comments in programs and that operators and users maintain current backup tapes and diskettes.

All to often a program is designed, coded, tested and then installed. When a bug is discovered, or a change is made, or the power goes out, the importance of documentation becomes real for the first time. Recreating programs, files and data can be avoided by the proper system documentation.

System documentation is not only for recovering from a crash. System documentation is just as important in maintaining or enhancing the program. When a change is made to a program, the original programmer is usually gone. Documentation is all you have and what you don't have will hurt you.

ENVIRONMENTAL CONTROLS:

The second major aspect of disaster recovery planning is environmental controls. The most common environmental control utilized is air conditioning in the data processing center. However, potentially more

damaging problems are in the electrical power supply.

These problems are not as rare as we might hope and there is something that you can do about it. Some authorities predict that the general quality of commercial power will decline rather than improve through the remainder of the century as demands increase and generating plants age.

It is commonly known that although power companies certainly don't like to take the blame for problems with customers' computer equipment, some utilities are beginning to accept that they are not supplying acceptable power to some customers.

According to Emergency Power Engineering, Inc., a vendor of computer power conditioning and backup equipment, computers' loads make up less than 1/2 of 1% of the total utility demand, reducing the utility's motivation to improve their power supply. However, some utilities have begun buying power equipment from vendors themselves and leasing the units to their sensitive power customers.

This arrives at a question of what you can do to keep your system up and running through blinks, brownouts, blackouts, droops or surges. A blink is a heavy loading line switch, meaning that your utility sometimes switches lines before the whole supply fails. Such a switch causes a half a second dip in power that's too fast for the human eye to perceive, but long enough to affect a computer. Brownouts are imposed voltage reductions and blackouts are unscheduled voltage

outage.

Whether an interruption of power is half a second or half a day, it can trigger an uncontrolled shutdown of your computer. That may mean the files and jobs that are open and active will be disrupted and take hours to rebuild. In the meantime, your accounting, purchasing, computer staffs and others who are dependent upon your computer system are idle and frustrated. This idle time and the time it takes to rerun jobs derailed in progress can be very expensive.

Data can also be damaged by shut downs in ways that are not immediately apparent. Heads in the act of writing from or to storage media may crash, destroying themselves, the media, and of course, the data. Even a brief gap in the power can interrupt critical communication and repeated gaps making even the best communication equipment unreliable.

The effects of some faults on equipments may not even be obvious or immediate. Delayed component failures may or may not be traceable to the transient's rapid voltage surges and droops that caused them. It may seem like bad luck, or blamed on the equipment itself.

The table on Voltage Tolerances of Computers is from the U.S.Department of Commerce. This chart lists the tolerances of most computer systems, the quality of most utility power and possible effects of running a computer on this power without protection.

The question again is, "What can you do to keep your system up and running through blinks, brownouts, blackouts." Results in some fairly straightforward measures that can help you provide for an orderly shut down in an extended power outage or smooth ride out of a brief interruption and can constantly condition the power supplies to your critical computer systems.

Just as the Civil Defense helps minimize the effects of natural disasters such as hurricanes providing an appropriate uninterruptible power supply (UPS) system for sensitive computers can make a difference between disaster and at least inconvenience. An UPS is basically a battery backup for your computer. Either On Line or Standby!

A Standby UPS is hooked on to the utility power but does not ordinarily do anything but monitor power. It does include a battery that holds a certain period's worth of reserve power. When the unit senses an interruption of power from the utility it sounds like an alarm and switches your system from a utility power to battery. You have until the battery runs out to power down in an orderly manner.

Although the Standby UPS are less expensive than On Line UPS, they do come with a possible danger of lag between the actual loss of utility power and the beginning to draw from the battery which may be long enough to cause damage in some systems.

An On Line UPS has its battery continually trickle charged by utility

power while an "inverter" converts the utility power to either D.C. power and back to A.C. power, finely regulated needs of computers.

The first thing you need to know to plan your own protection is what kind of power problems you face. Then obtain assistance from a computer manufacturer, computer power conditioning and backup equipment vendor. There is also a publication available from the U.S. Department of Commerce describing UPS systems and suggests down time may be reduced by as much as 50 to 60% after installation of an UPS.

SAFEGUARDS:

This section is on Safeguards. Managers charged with protecting data and computer hardware have a wide range of insurance options. However, it may be of interest to know what to insure!

There are different exposures to mainframes than there are to micros. The insurance industry reports that computer centers mainframes and minis have a real threat to water, smoke and fire. In fact, 35% of the claims involve water loss; vandalism and malicious damage account for 20% of the claims. In comparison to micro computers where 50% of the claims are theft and 33% of the losses are power surge related.

One could quickly conclude that micro computers because of their smaller size and unsecured location are uniquely prey to theft. The second greatest threat facing micros are power surges which harm the electronic components. Whatever the size of systems in use, as

reliance on computers continues to grow so does the need to protect computers.

A limited insurance policy can help plug the gaps in disaster recovery in risk management plans while extensive insurance coverage can provide virtual blanket coverage from damage of hardware to loss of software, data and storage media.

Insurance policies are written in two ways. All risk coverage protects the insured against any kind of mishap except those specifically excluded by the policy. By contrast, specific risk policies provide coverage only for occurrences that are spelled out in the contract. Generally, policies written for large systems are of the specific risk type while small system policies are usually all risk policies.

When buying insurance computer managers should not only consider the value of hardware and software they are insuring, but the data processing importance to the School District's bottom line on the costs involved in restoring, relocating computer equipment should a disaster strike. A comprehensive computer insurance program may include the following types of coverage:

Property The most fundamental type of coverage for computers. Property policies are common to systems of all sizes. Standard property coverage will protect computers but may not include such unique computer needs as power surges. Also, property insurance

generally will only cover the replacement cost of hardware and magnetic media, not the data and the programs that the magnetic media holds.

Business Interruption Most often referred to as loss of earnings coverage. Such policies cover loss of income an organization suffers because of computer failure. This may be of particular importance for Districts that are selling services to other school organizations.

Extra Expense This coverage pays for the actions an insured must take such as hiring programmers and consultants in order to restore computer operations after a systems failure or other problems. Insurance companies stress that business interruption and extra expense coverage are no substitute for proper data process procedure such as documentation, backing up data and planning for computers disasters, but are essentials of a computer policy!

Computer Crime This can be added to a blanket fidelity coverage for unauthorized computer access whether or not any crime is committed or intended.

Errors and Ommissions This is insurance for computer operations and consultants which covers the losses third parties may suffer because of insured School District's unintentional acts or as failure to act when it should.

Fidelity This insurance covers the dishonest acts of employees such

as illegally initiating fund transfers from school district to personal accounts.

As in the purchase of any insurance, the purchaser should be aware of depreciation versus actual cost replacement, deductibles and other coverage provisions which one may want to verify with their insurance consultant or risk manager.

A prudent manager, whatever the size of the computer system must realize that, as reliance on computers continues to grow, so does the need to protect computers, (both hardware and software) as well as personnel.

In summary, after crash, Use your disaster recovery plan and you will have a happy ending. Remember, "What you don't have will hurt you"!